DEPARTMENT OF THE NAVY
NAVY RECRUITING COMMAND
5722 INTEGRITY DR.
MILLINGTON, TN 38054-5057

COMNAVCRUITCOMINST 5211.4A
00J
18 Dec 2009

COMNAVCRUITCOM INSTRUCTION 5211.4A

From: Commander, Navy Recruiting Command

Subj: NAVY RECRUITING COMMAND PRIVACY PROGRAM

Ref: (a) 5 U.S.C. 552a
(b) DoD 5400.11 of 8 May 07
(c) DoD 5400.11-R of 14 May 07
(d) SECNAVINST 5211.5
(e) COMNAVCRUITCOMINST 5239.1
(f) COMNAVNETWARCOM VA 061635Z OCT 06
(g) DoNCIO 171952Z APR 07
(h) OPNAVINST 3100.6

Encl: (1) UNAUTHORIZED DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII) CHECKLIST

1. Purpose. To implement references (a) through (h). Ensure Navy Recruiting Command (NAVCRUITCOM) military members, civilian, and contractor employees are informed of their rights and responsibilities under the provisions of the Privacy Act of 1974 (PA). Balance the government's need to maintain information with the obligation to protect individuals against unwarranted invasions of their privacy stemming from Department of the Navy's (DoN's) collection, maintenance, use, and disclosure of Personally Identifiable Information (PII). Require the employment of privacy management practices and procedures to evaluate privacy risks in publicly accessible DoN websites and unclassified non-national security information systems.

2. Cancellation. COMNAVCRUITCOMINST 5211.4

3. PII. PII is defined as information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, social security number, birth date, home address, home phone number, or biometric records.

4. Rules of Conduct. All NAVCRUITCOM personnel shall be familiar with the responsibilities and duties imposed by references (a) through (e). Failure to comply with reference (a), may result in sanctions including reprimand,

suspension, removal, and/or civil and criminal penalties in accordance with applicable law and policy. At a minimum, any individual who demonstrates reckless disregard or a pattern of error in safeguarding PII will promptly have his or her access to information or systems containing PII revoked. In particular, the PA provides for criminal sanctions and fines of up to $5,000 against an official or employee who:

a. Willfully discloses information protected under the PA to an individual or agency not authorized access to it.

b. Willfully maintains a system of records that was not published in the Federal Register.

c. Requests, obtains, or receives personal data under false pretenses.

d. Fails to implement and maintain security controls, for which they are responsible and aware, for PII regardless of whether such action results in the loss of control or unauthorized disclosure of PII.

e. Fails to report any known or suspected loss of control or unauthorized disclosure of PII.

f. (For managers) Fails to adequately instruct, train, or supervise employees in their responsibilities.

5. Privacy Act Coordinator. The NAVCRUITCOM Staff Judge Advocate (00J) is appointed the Privacy Act Coordinator. Responsibilities include:

a. Develop overall NAVCRUITCOM policy relative to the PA.

b. Monitor and ensure compliance with Department of Defense (DoD) and Secretary of the Navy (SECNAV) PA instructions.

c. Develop materials such as forms, reporting formats, and directives for implementation of the PA. Consolidate data and make required reports, including denials of PA requests. Ensure training programs required by the PA are accomplished. Process requests and maintain processing logs for notification, access, and amendment under the PA. Coordinate with Navy Recruiting District (NAVCRUITDIST) and Navy Recruiting Region (NAVCRUITREG)

PA coordinators as required, and obtain assistance when necessary. Conduct or direct PA self-assessments as appropriate.

d. Lead the NAVCRUITCOM privacy team.

e. Within ten days of PII disclosure, coordinate the notification of all individuals affected by an unauthorized disclosure of PII. Issue notification letter, including specific data involved and the circumstances surrounding the incident. If unable to provide notification within ten days, the NAVCRUITCOM PA Coordinator shall notify DNS-36 of the delay in notification and the reason, and what actions are being taken to complete the notification. If unable to readily identify the affected individuals, a generalized notice should be sent to the potentially affected population, and establish a toll-free number (i.e., a Call Center) to allow impacted individuals the opportunity to obtain additional information regarding the loss. As part of any notification, individuals shall be informed to visit the Federal Trade Commission's (FTC's) web site at http://www.consumer.gov/idtheft for guidance on available protective actions.

6. Privacy Act Team. The PA team shall identify ways to prevent inadvertent releases of PII, review privacy protocols, and establish best business practices. Membership will include: the NAVCRUITCOM PA Coordinator (00J); Head, Management and Organizational Services (002SD); Director, Human Resources and Logistics (N1/N4); Director, Operations (N3); Director, Information Technology (N6); Public Affairs Officer, (00P); and the System Manager for each NAVCRUITCOM system of records.

7. Training. The NAVCRUITCOM PA coordinator, in conjunction with the NAVCRUITDIST and NAVCRUITREG PA coordinators, shall provide PA orientation training to new command personnel during check-in, and annual refresher training to all personnel. The NAVCRUITCOM PA coordinator will ensure specialized, management, and PA systems of records training is provided to appropriate personnel, as needed.

8. Safeguarding PII. The PA requires that safeguards be taken to ensure the security and confidentiality of PII contained in paper documents, electronic storage devices, electronic files, and systems of records.

a. Storage. During working hours, storage methods must ensure PII can only be viewed by those persons with an official need to know. Spaces in which PII is stored shall have limited access (i.e., locked doors, cabinets or drawers) after working hours.

b. Portable Storage Devices (PSDs). Per references (f) and (g), except for compelling operational necessities, the use of any PSD (floppy disks, compact discs, USB flash media drives or "thumb drives", etc.) containing PII is restricted to work places that meet storage standards in 7a. Any PSD containing 500 or more records of PII that is removed from such a work space shall be encrypted, properly marked, and signed in and out by a command representative. (R

c. Transmittal. In those instances where transmittal of PII is necessary, the originator must properly mark correspondence so receivers of the information are apprised of the need to properly protect the information. Documents or PSDs transmitted with PII (e.g. letters, memos, emails, faxed documents, recall rosters, etc.), shall be marked "FOR OFFICIAL USE ONLY (FOUO) - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

d. Disposal. Per references (c) and (d), PA records must be disposed by rendering the material unrecognizable or beyond reconstruction (e.g., burning, chemical decomposition, shredding, mutilation, etc.) The recommended method for disposal of paper PA records is via a cross-cut shredder. Never dispose of paper PA records in trash receptacles without first rendering them unrecognizable - trash bins are a common vulnerability for unauthorized disclosures.

e. Laptop Computers and Personal Digital Assistants. Extra caution must be used by personnel who maintain PII on laptop computers, blackberry devices, and similar mobile devices to ensure information is properly safeguarded against loss or compromise. Should a loss occur, ensure they are aware of the actions to take in the event of an unauthorized disclosure contained in paragraph 9 below. Any laptop computer or Personal Digital Assistant which contains PII shall also comply with the guidance in references (f) an (g), regarding PSDs. Reference (e) provides additional guidance for safeguarding laptop computers and the data stored on them. They must be signed in and out, be NIST certified, and encrypted. (R

9. Annual Review of Systems of Records. System managers will ensure each system of records under their cognizance complies with the PA, and, at a minimum, review each system of records annually to:

a. Determine if records from the system are used in matching programs and whether OMB Guidelines have been met.

b. Ensure the system of records, and each system notice in the Federal Register, is up-to-date (organization names, titles, addresses, etc., frequently change), label all system PII records "FOR OFFICIAL USE ONLY (FOUO) PRIVACY SENSITIVE."

c. Ensure the accuracy, relevancy, timeliness, and completeness of records that may be disclosed to anyone outside the federal government.

d. Stop the collection of PII that is no longer required and, when feasible, remove the information from existing records to reduce the "footprint" PII to the minimum necessary.

10. Unauthorized Disclosure. In the event of an unauthorized disclosure of PII, the activity shall take immediate action, as provided in references (c) and (d), and as implemented in enclosure (1).

11. NAVCRUITREG/NAVCRUITDIST PA Coordinators. Each NAVCRUITREG and NAVCRUITDIST shall appoint, in writing, a PA Coordinator for their activity. Copies of the letters of appointment are to be mailed to NAVCRUITCOM PA Coordinator. The NAVCRUITREG/ NAVCRUITDIST PA Coordinator shall serve as the point of contact for all PA matters for their activity. Specific duties include: respond promptly to requests from the NAVCRUITCOM PA Coordinator, provide orientation and annual refresher PA training to their activity personnel by utilizing material provided by the NAVCRUITCOM PA Coordinator, and ensure PII is properly safeguarded.

12. Reporting Requirements. Unit situational reports will be released immediately upon notification of unauthorized disclosure of PII. Enclosure (1) provides reporting guidelines. Report Control Symbol 5211-1 has been assigned to this requirement.

/s/
R. L. GRAF
Deputy

Distribution:
Electronic only via
http://www.cnrc.navy.mil/Publications/directives.htm

UNAUTHORIZED DISCLOSURE OF PROTECTED PERSONAL INFORMATION (PPI) CHECKLIST

1. Unauthorized Disclosure. Take immediate action to recover PII and prevent further loss, damage, or disclosure.

2. Informal Report. Immediately notify NAVCRUITCOM PA Coordinator (00J) of unauthorized disclosure. Forward the following information to NAVCRUITCOM PA Coordinator as it becomes available:

a. Component/organization involved (NAVCRUITREG, NAVCRUITDIST, etc.).

b. Number of individuals impacted, and whether they are government employees or private citizens (if both, provide percentage of each).

c. Brief description of the incident, including the date of incident, circumstances of the breach and PPI lost or compromised.

d. Description of the remedial efforts, including any notifications made to the individuals whose information was compromised.

e. Do not delay notification to the PA Coordinator. If some information is not yet known, provide the available information, and send follow up reports when additional information is obtained. This notification should happen as soon as possible, but in no circumstance should it take greater than 24 hours to complete notification.

f. The PA Coordinator will, in turn, notify Chief of Naval Operations (CNO) (DNS-36) via email within 24 hours with “Identity Theft Notification” in the subject line, with a synopsis of the disclosure made, number of individuals affected, actions taken, and actions to be taken. COMNAVCRUITCOMNOTE 5239 contains additional reporting requirements if the compromise involves the lost or theft of computer equipment.

3. Formal Report. Review OPNAVINST 3100.6, Special Incident Reporting Procedures, and notify the NAVCRUITCOM PAO. Issue an OPREP 3 Navy Blue if an incident could or will attract national media attention. If an OPREP 3 Navy Blue is not required, do not send an OPREP 3 Unit Sitrep; instead, continue to provide

information to the NAVCRUITCOM PA Coordinator in accordance with informal reporting requirements, paragraph 2 above.

4. Identity Theft Notification. Activities must provide the names and complete, accurate addresses of all affected individuals to the NAVCRUITCOM PA Coordinator, who, within ten days, shall notify all affected individuals by letter, including the specific data involved and the circumstances surrounding the incident. If unable to provide notification within ten days, notify DNS-36, via the NAVCRUITCOM PA Coordinator of the delay in notification and the reason, and what actions are being taken to complete the notification. If NAVCRUITCOM is unable to identify the affected individuals, a generalized notice will be sent to the potentially affected population. When affected personnel cannot be located or directly contacted, establish a toll-free number (ie, a Call Center) to allow impacted individuals the opportunity to obtain additional information regarding the loss. As part of any notification, individuals shall be informed to visit the Federal Trade Commission's (FTC's) web site at http://www.comsumer.gov/idtheft for guidance on available protective actions.